



# *Security Log's Training Guide*

*Broadsword Program Office  
Air Force Research Laboratory /  
315-330-4429*

## ISSO



## Services



- Audit Logs
  - Create Audit Report based on:
    - User Name
    - Event Type
    - Date Range
  - Archive Audit Logs
  - Remove Archived Logs
- Archived Logs
  - Query Archived Logs based on:
    - User Name
    - Event Type
    - Date Range

ISSO

Audit Logs

The purpose of this screen is to allow the ISSO to view, archive, or remove audit information from the Broadsword Sybase Data Base based on user(s), date/time and audit event.

The Audit Log Maintenance screen contains a table of parameters. The first four parameters are used to query for the audit information, the last parameter is used when archiving the audit information.

**Audit Logs**

**Audit Log Maintenance** Help

User :

Start Date :

End Date :

Event :

Archive File Name :

Audit Report Archive Records Remove Records Reset

**Annotations:**

- The user account being queried for audit information. The end date/time of the audit information being
- The start date/time of the audit information being
- The audit event being queried.
- Name of file queried to contain audit records being archived. (The directory path is not included in the filename.)
- Request an audit report for viewing based on the query parameters selected in the parameter table.
- Archive the records returned from the query based on the parameters selected in the parameter table.
- Remove the records from the Broadsword Sybase Data Base that are returned from the query based on the parameters selected in the parameter table.
- Returns the selections to their previously applied values and automatically applies these changes.

ISSO

• Audit Logs

Example:

The ISSO for our local system wants to get a report on user 'test05'; in particular he wants a record of every log-in attempt by this user. The information filled in on the right specify the correct query. All the ISSO needs to do is click the Audit Report button.

The Audit Log Maintenance screen contains a table of parameters. The first four parameters are used to query for the audit information, the last parameter is used when archiving the audit information.

The user account being queried for audit information. The end date/time of the audit information being

Name of file queried to contain audit records being archived. (The directory path is not included in the filename.)

Request an audit report for viewing based on the query parameters selected in the parameter table.

Archive the records returned from the query based on the parameters selected in the parameter table.

Remove the records from the Broadsword Sybase Data Base that are returned from the query based on the parameters selected in the parameter table.

Returns the selections to their previously applied values and automatically applies these changes.

**Audit Logs**

**Audit Log Maintenance** Help

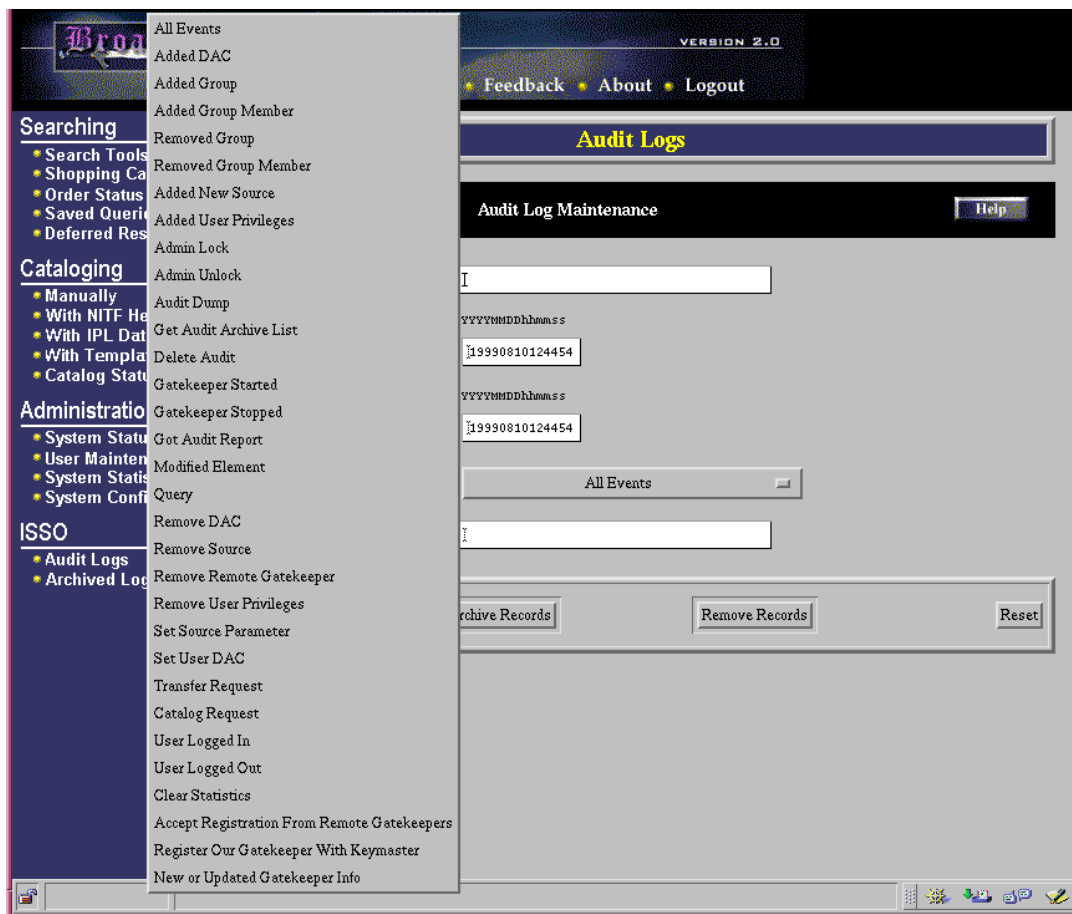
<b>User :</b>	<input style="width: 80%;" type="text" value="test05"/>
<b>Start Date :</b>	<input style="width: 80%;" type="text" value="YYYYMMDDhhmmss 19990505182022"/>
<b>End Date :</b>	<input style="width: 80%;" type="text" value="YYYYMMDDhhmmss 19990505182022"/>
<b>Event :</b>	<input style="width: 80%;" type="text" value="User Logged In"/>
<b>Archive File Name :</b>	<input style="width: 80%;" type="text"/>

Audit Report
Archive Records
Remove Records
Reset

ISSO

• Audit Logs

This is a listing of all the audit events that the ISSO can select for the audit report. The default is All Events.



ISSO

Audit Logs

This screen is the result of clicking on the Audit Report button from the previous page. By clicking on the "View Audit Report" link, the user can view the audit report generated by the criteria specified.

Example: This screen means that the previous request for all log-in information on user test05 up to May 5, 1999 has been processed, and that a report has been generated. To view the report, all the ISSO has to do is click on the "View Audit Report" hyperlink.

**Audit Log Maintenance**
Help

<b>User :</b>	<input style="width: 80%;" type="text" value="test05"/>
<b>Start Date :</b>	<div style="border: 1px solid black; padding: 2px;"> <small>YYYYMMDDhhmmss</small>  19990505000000 </div>
<b>End Date :</b>	<div style="border: 1px solid black; padding: 2px;"> <small>YYYYMMDDhhmmss</small>  19990505235959 </div>
<b>Event :</b>	<div style="border: 1px solid black; padding: 2px;"> User Logged In </div>
<b>Archive File Name :</b>	<input style="width: 100%;" type="text"/>

[View Audit Report](#)

Audit Report
Archive Records
Remove Records
Reset

Link to audit report generated using the current search criteria.

ISSO

• Audit Logs

This is the report header. It contains all of the audit log criteria specified in the previous screen.

This is a sample audit report generated by the "Audit Log Maintenance" page.

Example:

This is the log generated by the previous request. The header contains all of the log criteria, and the rest contains log entries.

## Audit Report

User: test05 Starting at : 19990505000000 and Ending at : 19990505235959 For Event: LOGIN

Login: test05 IP: 123.456.7	Orig. Login: test05 Gtkey:	Session Key: 10205
LOGIN @ 19990505185343 : Successful Login from sun Gatekeeper		
Login: test05 IP: 123.456.780	Orig. Login: test05 Gtkey:	Session Key: 10652
LOGIN @ 19990505194650 : Successful Login from sun Gatekeeper		

This is a sample log entry. Each entry contains the username, IP Address, Gatekeeper, and Session Key, as well as all of the events that were audited.

ISSO

• Audit Logs

This screen is a result of clicking the “Archive Records” button on the “Audit Log Maintenance” page.

Example: Now, let us suppose that the ISSO wants to archive the report that he just generated. By clicking on the “Archive Records” button, the ISSO can archive the report in a file called audit050599.

Audit Logs

Audit Log Maintenance Help

User :	<input type="text" value="test05"/>
Start Date :	<div>YYYYMMDDhhmmss</div> <input type="text" value="19990505182022"/>
End Date :	<div>YYYYMMDDhhmmss</div> <input type="text" value="19990505182022"/>
Event :	<input type="text" value="User Logged In"/>
Archive File Name :	<input type="text" value="audit050599"/>

Archived record(s) successfully.

Audit Report
Archive Records
Remove Records
Reset

This is the confirmation message from a request to archive a record.

ISSO

• Audit Logs

Example:

Let's say that the ISSO now wants to remove the audit050599 record. After entering the filename and clicking the "Remove Records" button, this confirmation screen appears. Clicking on the "Remove Records" button again will confirm the removal.

This is the warning displayed when a remove record request is made.

Audit Logs

Audit Log Maintenance Help

User :	<input type="text" value="test05"/>
Start Date :	<input type="text" value="YYYYMMDDhhmmss"/> <input type="text" value="19990505182022"/>
End Date :	<input type="text" value="YYYYMMDDhhmmss"/> <input type="text" value="19990505182022"/>
Event :	<input type="text" value="User Logged In"/>
Archive File Name :	<input type="text" value="audit050599"/>

**WARNING: Verify Record Deletion by Clicking Remove Records Again.  
These Records will be PERMANENTLY Removed from the System.**

Audit Report
Archive Records
Remove Records
Reset

ISSO

Audit Logs

Example:

After clicking on the "Remove Records" button, the ISSO receives confirmation that the file audit050599 has been removed.

This page confirms the removal of an archive.

Audit Logs

Audit Log Maintenance Help

User :	<input type="text" value="test05"/>
Start Date :	YYYYMMDDhhmmss <input type="text" value="19990505182022"/>
End Date :	YYYYMMDDhhmmss <input type="text" value="19990505182022"/>
Event :	<input type="text" value="User Logged In"/>
Archive File Name :	<input type="text" value="audit050599"/>

Removed record(s) successfully.

Audit Report
Archive Records
Remove Records
Reset

This is the confirmation message from a request to remove a record.

## ISSO

- Audit Logs
- Archived Logs

.....

This page displays a listing of all the archived files that the user can select and view.

Archived Logs		
SELECT	ARCHIVE FILE	DATE ARCHIVED
<input type="checkbox"/>	security_test	19990505113638
<input type="checkbox"/>	diane	19990505175035
<input type="checkbox"/>	audit050599	19990505182550

Audit Archive Queries		Help
User :	<input type="text"/>	
Start Date :	YYYYMMDDhhmmss <input type="text" value="19990505185445"/>	
End Date :	YYYYMMDDhhmmss <input type="text" value="19990505185445"/>	
Event :	<input type="text"/>	
<input type="button" value="Query Archives"/>		

## ISSO

- Audit Logs
- Archived Logs

### Example #1:

ISSO selected the archived file audit050599 to query and view *all events* for the user *test05*.

### Archived Logs

SELECT	ARCHIVE FILE	DATE ARCHIVED
<input type="checkbox"/>	security_test	19990505113638
<input type="checkbox"/>	diane	19990505175035
<input checked="" type="checkbox"/>	audit050599	19990505182550

### Audit Archive Queries

User :

test05

Start Date :

YYYYMMDDhhmmss

19990505185445

End Date :

YYYYMMDDhhmmss

19990505185445

Event :

All Events

Query Archives

Help

## ISSO

- Audit Logs
- Archived Logs

### Example #2:

ISSO selected the archived file *security\_test* to query and view *user login* information for *all users*.

Note: When the user field is left blank the default is *all users*.

### Archived Logs

SELECT	ARCHIVE FILE	DATE ARCHIVED
<input checked="" type="checkbox"/>	security_test	19990505113638
<input type="checkbox"/>	diane	19990505175035
<input type="checkbox"/>	audit050599	19990505182550

### Audit Archive Queries

User :

Start Date :

YYYYMMDDhhmmss

19990506191746

End Date :

YYYYMMDDhhmmss

19990506191746

Event :

User Logged In

Query Archives